## IN THE CLAIMS

1. (original) A method of controlling distribution of a segment of encrypted electronic information, comprising:

receiving, from a key server, a protected decryption key associated with the segment;

retrieving, at a user location, the segment;

obtaining an unprotected copy of the decryption key from the protected decryption key;

decrypting, in response to said obtaining, the segment using the unprotected copy of the decryption key;

destroying the unprotected copy of the decryption key at the user location in response to said decrypting;

displaying the decrypted segment in response to said decrypting; and

destroying the decrypted segment in response to said displaying.

2. (currently amended) The method of claim 1, further comprising:

saving, in response to said receiving, the protected decryption key;

wherein said destroying the unprotected copy of the decryption key does not effect the ~~unprotected~~ protected copy of the decryption key.

3. (original) The method of claim 1, further comprising:

said receiving further comprising receiving at least one access policy associated with at least one of the key server, the user location, the segment, the decryption key, and a user, the at least one access policy including at least one fixed time limitation;

said determining comprising determining whether current operating conditions, including the current time, satisfy the at least one access policy.

4. (original) The method of claim 1, further comprising:

saving, in response to said receiving, the protected decryption key in memory; and

rendering the protected copy of the decryption key inaccessible after an expiration time in the at least one access policy.

5. (original) A method for issuing a key lease, comprising:

receiving, at a remote server, a request to lease a decryption key for an encrypted electronic segment;

determining whether a key lease can be issued for the encrypted electronic information based on at least one of a remote server restriction, an information restriction, and a user restriction;

creating a voucher in response to a determination that the key lease can be issued, said voucher including at least the decryption key, and at least one time limitation associated with the decryption key;

encrypting at least the decryption key of the voucher; and

sending the voucher to the user location.

6. (original) The method of claim 5, wherein said creating further comprises adding access policies associated with the information to the voucher.

7. (original) The method of claim 5, wherein said receiving further comprises receiving a requested time frame of use of the key lease, and wherein the at least one time limitation includes an expiration time based on at least one of a maximum allowed by the remote server, a maximum allowed by the information, a maximum allowed by user limitations, and the requested time frame.

8. (original) The method of claim 5, further comprising:

said encrypting utilizing a first information from the user location and a second information from the remote server; and

said sending further comprises sending the second information to the user location;

wherein the second information is insufficient in and of itself to decrypt the voucher.

9. (original) The method of claim 5, further comprising destroying the decryption key at the remote server after a predetermined period of time.

10. (currently amended) The method of claim ~~5~~ 1, further comprising:

logging said obtaining in a log; and

sending, from the user location to a remote server, the log.

11. (original) The method of claim 10, further comprising logging a time of said obtaining in the log.

12. (original) A method of controlling distribution of electronic information, comprising:

sending, from a user location to a key server, a request to access a protected segment, and a first information;

receiving, at the user location from the key server, an encrypted voucher and a second information, said voucher including at least a decryption key associated with the segment;

retrieving, at a user location, the segment;

obtaining a decrypted copy of the decryption key using the first and second information;

accessing, in response to said decrypting, the segment using the at least a portion of the voucher;

destroying, in response to said accessing, the decrypted copy of the decryption key.

13. (original) The method of claim 12, further comprising:

displaying the accessed segment in response to said accessing; and

destroying the accessed segment in response to said displaying.

14. (original) The method of claim 12, wherein the voucher includes access policies, the method further comprises:

determining, in response to said decrypting, whether operating parameters satisfy the access policies; and

said accessing being responsive to said operating parameters being determined to satisfy the access policies;

wherein said accessing is responsive to said decrypting through said determining.

15. (original) A method for controlling distribution of electronic information, comprising:

retrieving, at a user location, a segment of encrypted electronic information;

receiving, from a key server, an encrypted decryption key for the segment;

saving said encrypted decryption key in a memory;

obtaining a decrypted copy of the decryption key in response to an authorized user request to access the segment;

accessing the segment using the decrypted copy of the decryption key at the user location for the segment; and

destroying the decrypted copy of the decryption key at the user location in response to said accessing without destroying the encrypted decryption key in memory.

16. (original) The method of claim 15, further comprising:

displaying the decrypted segment in response to said accessing; and

destroying the decrypted segment in response to one of said displaying.

17. (original) A method of accessing a protected segment of electronic information, the segment having an associated key, comprising:

retrieving, at the user location, the segment;

receiving, at the user location from the remote server, the key;

accessing the segment, in response to said receiving, using the key;

displaying the segment as accessed;

destroying the key in response to one of said displaying and said accessing, wherein the key is ~~never~~ only momentarily stored in memory at a user location between said receiving and said destroying;

receiving, at the user location from the remote server, an encrypted key lease including the key;

saving the encrypted key lease in a memory;

breaking a connection between the user location and the remote server; and

during a period of the broken connection:

retrieving, at the user location, the segment;

obtaining a decrypted copy of the key from the key lease;

accessing the segment in response to said obtaining;

displaying the segment as accessed; and

destroying the decrypted copy of the key in response to one of said displaying and said accessing.

18. (original) The method of claim 17, further comprising restoring a connection between the user location and the remote server.

19. (original) The method of claim 18, further comprising revoking the key lease after said restoring.

20. (original) The method of claim 18, further comprising:

logging said obtaining in a log; and

sending, after said restoring, the log from the user location to the remote server.

21. (original) The method of claim 20, further comprising detecting, at one of the user location and the remote server, from the contents of the log, any tampering at the user location relating to at least one of the key lease, the segment, and operating conditions at the user location.

22. (original) A method of viewing a segment of encrypted electronic information on a display, comprising:

receiving, from a remote server, an encrypted decryption key for the segment;

retrieving, at a user location, a segment of encrypted electronic information;

first decrypting the encrypted decryption key in response to the presence of authorized conditions;

second decrypting the segment using the decrypted decryption key;

destroying, at the user location, all copies of the decrypted decryption key in response to said second decrypting, without destroying the encrypted decryption key;

displaying the segment as decrypted on the display; and

destroying, at the user location, the segment as decrypted in response to said displaying.

23. (original) A method of controlling distribution of a segment of encrypted electronic information, the segment having a first and second portion, the method comprising:

receiving, from a key server, an encrypted voucher, the voucher including first and second decryption keys associated with the first and second portions, respectively,

retrieving, at a user location, the segment;

accessing the protected copy of the first decryption key;

decrypting, in response to said accessing, the first portion of the segment using the accessed copy of the first decryption key;

destroying the accessed copy of the first decryption key at the user location in response to said decrypting;

displaying the decrypted segment in response to one of said decrypting and said destroying;

destroying the decrypted first portion in response to said displaying;

accessing the protected copy of the second decryption key after said destroying the first decrypted segment; and

decrypting, in response to said accessing the protected copy of the second decryption key, the second portion of the segment using the accessed copy of the second decryption key.

24. (currently amended) A method of limiting access to a segment of encrypted information, comprising:

saving, at a remote server, a decryption key for the segment, the segment being at a location other than the remote server;

receiving a request from an authorized user for the decryption key;

sending a copy of the decryption key from the remote server to a source of the request;

destroying the decryption key at the remote server in response to the elapse of a predetermined period of time; and

preventing the source from retaining the copy of the decryption key, wherein said destroying leaves said segment permanently inaccessible absent breaking of the encryption protecting of the segment.

25. (canceled).

26. (original) A system for accessing a protected segment of electronic information, comprising:

means for receiving, from a key server, a protected decryption key associated with said segment;

means for retrieving, at a user location, said segment;

means for obtaining an unprotected copy of said decryption key from said protected decryption key;

means for decrypting, in response to said obtaining, said segment using said unprotected copy of said decryption key;

means for destroying said unprotected copy of said decryption key at said user location in response to said decrypting;

means for displaying said decrypted segment in response to said decrypting; and

means for destroying said decrypted segment in response to said displaying.

27. (original) The method of claim 26, further comprising:

means for saving, in response to said receiving, said protected decryption key;

wherein said means for destroying said unprotected copy of said decryption key does not effect said unprotected copy of said decryption key.